ArubaOS™ Mobility Controller Software

2.4.0.0 Release Notes

Copyright © 2005 Aruba Wireless Networks, Inc. All rights reserved. Specifications in this document are subject to change without notice. Originated in the USA.

AirOS, Aruba 5000, Aruba 2400, Aruba 800, Aruba 60/61, and Aruba 70 are trademarks of Aruba Wireless Networks, Inc. in the United States and certain other countries. Any other trademarks appearing in this document are the property of their respective companies.

What's New in Release 2.4.0.0

These release notes describe new features in ArubaOS[†] 2.4.0.0 including:

- Licensing
- External Services Interface
- Client Integrity Module for Sygate Remediation
- 2E Wired Access Point
- 800-E and 2400-E Access Point Concentrators
- A6000 (Supervisor II)
- xSec Encryption
- Adaptive Radio Management
- Open XML Interface
- Configurable NAS IP addresses
- Secure LDAP

The following features are included in this release:

Licensing

As of ArubaOS 2.4, product licenses will enable the following features:

- Policy Enforcement Firewall
- VPN Server
- Wireless Intrusion Detection
- Advanced AAA
- External Services Interface
- Client Remediation Module
- Remote Access Points
- xSec Module

There are two types of licenses available:

1. A permanent license obtained at the time the feature was purchased
2. A trial license which is a temporary license available upon request for the purpose of evaluating a feature prior to purchase

For more information about licensing, refer to the *Managing Software Feature Licenses* (p/n 0500100-01) which is included with your switch.

WARNING

When license keys are enabled on your wireless LAN switch, abnormal tampering of the switch's system clock (setting the system clock back by 2 hours or more) will result in the "Disabling" of temporary licensed software modules and their supported features. This can be network service effecting. Aruba recommends that you make necessary clock adjustments prior to installing temporary license keys.

[†] As of Release 2.4, Aruba is renaming the OS to ArubaOS. Releases lower than 2.4 will continue to be referred to as AirOS.

ESI

The Aruba External Services Interface (ESI) provides an open interface to integrate security solutions that solve interior network problems such as viruses, worms, spyware, and corporate compliance. ESI permits configuration of different server groups— each group potentially performing a different action on the traffic. The Aruba ESI can be configured to do one or more of the following for each group:

- Perform health checks on each of the servers in the group
- Redirect specified types of traffic to the server
- Perform per-session load balancing between the servers in each group
- Provide an interface for the server to return information about the client that can place the client in special roles such as “quarantine”

Sygate Remediation

Sygate provides software-based solutions to enforce host remediation policies for different kinds of users. For clients/devices that are under the control of the IT administrator, the Sygate Security Agent is installed on the client computer. The Aruba switch integrates with the Sygate On-Demand Manager to enforce client/host integrity policies and to ensure that the agent is kept up to date (anti-virus patches, software updates etc.).

Most enterprise networks also have clients that are not under the control of the IT administrator (such as guest computers) and therefore client software cannot be pre-installed on these machines. For cases such as these Sygate offers the Sygate On-Demand Agent. This Agent can be uploaded on an Aruba switch and downloaded on the client machine to implement host integrity checks, and other functions such as Virtual Desktop, before allowing the client to be authenticated and allowed access to the network.

2E Wired Access Point

The Aruba 2E is a low-cost, two-port wired access point. It is designed to secure network traffic from a user port across an IP network to an Aruba access controller, where security services are applied to all user sessions.

The Aruba 2E appears as a transparent bridge to an end user device, such as a PC or an Ethernet hub, and as an IP endpoint to the rest of the network. When connected to an IP network, the Aruba 2E transparently establishes a GRE or IPSec tunnel over the network to automatically locate an Aruba access controller. All user traffic is securely passed over this tunnel to the Aruba mobility controller.

800-E and 2400-E Access Point Concentrators

The 800-E and 2400-E are wired security Access Points that will deployed in the closet distribution switch to secure network ports located either in common areas, conference rooms or cubes, and office ports. All traffic traversing the 800-E and 2400-E will be aggregated into a tunnel and backhauled over the network to an Aruba switch, where security services will be applied.

The 800-E supports:

- 8 x 10/100 MDI/MDX FE ports that provide user connectivity to the network
- 1 x 1000 Ethernet network uplink port

The 2400-E supports:

- 24 x 10/100 MDI/MDX FE ports that provide user connectivity to the network
- 2 x 1000 MDI/MDX Ethernet network uplink port

A6000 (Supervisor Card II)

The Aruba 6000 mobility controller is equipped with a two-port gigabit Ethernet line card and a supervisor module capable of processing up to 3.6 Gbps of encrypted traffic. Aruba's 6100 mobility controller is capable of supporting up to 7.2 gigabits of encrypted throughput and comes equipped with two line cards and two supervisor modules. All existing Aruba WLAN switches can be easily transformed to Aruba Mobility Controllers by upgrading from Aruba AirOS to Aruba's new ArubaOS thereby delivering investment protection for existing Aruba customers.

Aruba mobility controllers also provide application-based redirection and load balancing. This provides better optimization of security services such as anti-virus firewalling. Because Aruba mobility controllers provide deep packet inspection, only traffic that requires filtering is sent to anti-virus, content scanning or end-point remediation servers.

xSec Encryption

Extreme Security (xSec) is a unique and new encryption security protocol developed jointly by Aruba and Funk systems that provides advanced encryption at Layer 2 using AES. xSec is designed for high-level security compliance required for Federal communications.

xSec is a software licensed module within ArubaOS 2.4. New within the xSec module for ArubaOS 2.4 is:

- xSec Client – Server Encryption

  xSec client-server on the Aruba mobility controller provides termination of xSec client sessions from supplicants residing on the users PC. Additionally, xSec provides a uniquely non disruptive upgrade overlay solution for 802.11i / WPA2 for legacy infrastructure that is incapable of supporting the new standard natively.

- xSec Point – Point Encryption

  In addition to client-server deployments, xSec supports the ability to encrypt trunk ports on Aruba mobility controllers (Point-Point xSec), securing traffic between Aruba platforms at Layer 2.

Adaptive Radio Management

Adaptive Radio Management (ARM) has been enhanced to provide additional functionality for Air Monitoring and Voice quality of service as follows:

Multi-band Scanning—provides configurable AP based Air Monitoring channel and band scanning capability. With multi-band scanning, an AP can service WLAN clients on a specified frequency band and simultaneously scan additionally supported bands as an Air Monitor for interference, rogue or ad-hoc network activity on the alternate band.

Voice-aware Scanning—provides additional class of service / quality of service support for Wi-Fi Voice over IP stations, ensuring Voice sessions are given priority service in access to the available network resources. When ARM is performing RF scanning or Air Monitoring transactions, it now listens for Voice control session setup requests; protocols supported include

Vocera, SCCP, SVP and SIP. As one of these sessions is detected, ARM will cease RF scanning for the voice detected area in the network to enable maximum available resource to priority handle the call setup and session thought the duration of the call.

Open XML Interface

Supported in the Aruba Advanced AAA software module, ArubaOS 2.4 supports an open XML which allows integration with 3rd party servers and devices with the Aruba mobility controller using a standard XML language.

Configurable NAS IP addresses

This capability enhances the Aruba wireless security solution for wholesale or service provider environments in providing support to configure a specifically reported NAS IP address differently to each back-end AAA server.

Secure LDAP

Support for SSL encrypted transport and transactions between an Aruba WLAN Mobility Controller (WLAN switch) and LDAP servers.

Naming Changes

With this release, the following name changes have been made:

- Aruba WLAN Switches are now called Mobility Controllers. '
- The **show log arubaauth** command is now **show log authmgr**
- **var/log/arubalog** on mobility controllers is now **var/log/oslog**
- **arubamsg** in packet-filter commands is now **sysmsg**
- The **show aaa ap aruba-ap** command is now **show aaa ap managed-ap**
- **aruba_filter** has been renamed to **packet_filter**
- **aruba_ntpd** has been renamed to **ntpwrap**

Known Issues and Limitations in this Release

The following features and functionality have the following issues for Release 2.4.0.0. Where bug IDs are applicable, they are included in the description of the issue, and an expiration timer for local user database accounts.

- If a line card is removed and the switch is rebooted before the line card is replaced, the VLAN configuration reverts to default values. (6226)
- Enabling NAT for source addresses on Aruba switches is compatible with Nortel VPN clients provided a rule is added before the src-nat rule. To support RSA token and time syncing, specify a rule on the client firewall.
- Access Points that are indirectly connected to Aruba Mobility Controllers through third-party switches may have problems processing IP packets larger than 1500 bytes. Aruba recommends setting the maximum transmission unit (MTU) on these Access Points to 1500 bytes. Do this by entering (from enable mode) under the AP location:
  ap location 0.0.0 mtu 1500
  write memory
- Aruba only supports directly connecting Aruba Mobility Controllers with a cross-over cable. Connecting Aruba Mobility Controllers with straight-through cables is not recommended. Using the proper (cross-over) cable, ports on both sides of the connection can be configured to auto-negotiate or can be hard coded as long as they match.

- The user entry created on the Home Agent (HA) does not display the correct Location, Roaming, ESSID/BSSID/Phy values even though mobility sends the right values to Auth. (This is a display-only issue,) (6151)
- If after upgrading from ArubaOS 2.0.x to 2.4.0.0, you notice that some Ethernet ports fail to come up, check the port setting. It is likely these ports are configured as 100/10 half or full duplex when they should be set to auto-negotiate. (The port configuration mechanism for 2.2.4.0.0 differs from that in 2.0.x which may cause occasional port misconfigurations.)
- Devices that are idle for extended periods of time (for example, overnight) but which need to maintain their connection to an Aruba switch, must be able to respond to ICMP requests from the Aruba switch. However, the default settings of many personal firewalls, (including XP SP2), deny incoming ICMP requests. This configuration results in the devices experiencing frequent disconnects and reconnects, as well as DHCP address problems. To eliminate connection problems, be sure to configure firewall settings to allow ICMP requests from the Aruba switch.
- Many personal firewalls and ad/pop-up blocker programs, (for example Google and Yahoo) block pop-up windows by default. This can cause Captive Portal logon/logout issues if the switch URL does not explicitly allow pop ups. To prevent this problem, allow pop ups for the switch's URL.
  To log-out from a Captive Portal session if the pop-up window is not available, point your web browser to:
  http://<switch ip address>/auth/logout.html

- In deployments with the Aruba dialer and RSA SecurID, new/next pin mode RSA token time syncing support requires that the Aruba dialer be added into the firewall's application exception list. (For more information on configuring a firewall application exception list, refer to the Microsoft knowledge base, as this is typical for Microsoft applications.) This step is not required for normal operations.
- The Microsoft XP SP2 personal firewall already allows L2TP whereas Sygate needs this to be configured manually.
- RF Plan is a view-only application in MAC OS.
- Occasionally, in-band destined traffic is routed through the out-of-band (mgmt) interface. (6629)
- User entries showing wrong Location and Roaming Status may occur after a failover and recovery. The HA shows the correct information but the FA may not. (6858)
- While moving a station, if 802.1x authentication is delayed, the **show user global-user-map** command output is not displayed correctly. (6557)
- Wired clients who fail authentication are blacklisted, but they can still try to login. (6802)
- Session mirroring does not update for sessions that are already up. (6829)
- All PPTP connections to Aruba (or any PPTP server) for users with Windows XP Service Pack 2 firewall enabled, will experience a one minute wait before being able to reconnect.
- If trim-fqdn is enabled for 802.1x server, the domainname portion for the FQDN is still passed to the RADIUS server by the client internal EAP module. (6898)
- If the username is in the format of domain\username, trim-fqdn does not remove the domain portion before sending request to the server. (6804)
- There is a BW contract granularity limitation. The effective bandwidth enforced is not accurate for contracts less than 300 Kbits. (6838)
- The wired-dot1x role-based VLAN is not supported for SecureJack. (7464)
- WiFiMUX wired 802.1x is not supported in this release. 6310)
- Remote APs are not notifying the switch when they reboot so the switch can properly take down the IPSec tunnel connection. (5897)
- Changes in the NTP Servers list on master switches are not being propagated to local switches. (4944)
- If you are not doing any backend or local database authentication for administrative users, Aruba recommends that you disable this feature by using the **aaa mgmt-authentication mode disable** command.

- To restore the correct syslog facility level from a saved configuration file, do a **write erase** before executing a **copy flash: <saved-cfg> flash: default.cfg**.
- ESI can be used within a multi-switch topology with master and local switches and full redundancy. However, the following limitations apply in this release.

    1. On the WebUI, using the **Back** button to move back to previous browser pages occasionally causes incorrect data, (blanks) to be filled in some fields. This can result in ESI misconfigurations being sent to the switch. (7618).
    2. By design, in a multi-switch topology, client VLANs should not be shared across switches. For example, client VLAN 100 cannot be configured on switch lms1 and lms2 as doing so would cause the AVF routes to be incorrect when the client moves between the switches. Use separate VLANs instead on each switch and let mobility take care of preserving the IP addresses of the client when the client moves between switches.
    3. By design, multi-switch topology will only work in route mode. Bridge mode requires the AVF servers to be directly connected to the Aruba switch as server up/down status is detected by the port link status.
    4. In redundant switch configurations, do not use bridge mode. Use route mode to keep redirected packets properly forwarded. (7912)

- After a role-based VLAN is disabled, the 802.1x client will not have connectivity for a few minutes. (7892)
- **Monitoring > Switch Summary** may not display the correct total of clients and switches. The WLAN client summary may be smaller than the total of client entries because the per-switch display includes additional entries – which are not shown in the global user list. (7904)
- When you upload a license certificate, fpweb will restart. This is normal. However, the restart event is incorrectly logged as an fpweb crash. You can ignore this log message. (7940)
- When uploading a certificate while using a non-supported browser, you may receive a message that the “document contains no data”. You can typically ignore this message. However, Aruba recommends that you only use IE. 7928)
- After restoring a configuration, verify that your logging levels are set properly as they may not be restored. (7542)
- If you have licensed features on a Supervisor Card and need to replace that card, be sure to restore the configuration from backup on the new card to restore your license information. For more information, refer to the *Managing Software Feature Licenses* document that ships with your switch.
- Using A60/61 APs with Cisco 3550 PoE switches requires the Cisco switches to running IOS 12.1 (19) or later. Aruba recommends that you also make the following configuration settings on the Cisco 3550 (INLINE POWER) port:
    - power inline delay shutdown 15 initial 25
    - (config-if) spanning-tree portfast
- The 800-E and the 2400-E Gigethernet ports only support 1000Base-T rates.
- In this release, if the logging level of authmgr (formerly known as arubaauth) is set to a non-default level, when the Switch is upgraded to 2.4, the logging level is changed to the default level of Informational. (7959)
- Sygate SODA users should note that upload file names cannot contain spaces.
- Wired clients appear on All WLAN Clients pages in the WebUI .(7968)
- Redundancy will not work if VRRP is run over an encrypted link between switches using xSec PTP. (7472)
- Funk-Odyssey clients may experience delays in getting authenticated when using WPA encryption and server derivation roles where the VLAN of the client is set by matching a particular attribute. Aruba recommends that these users set the WPA Key Timeout and WPA Retry Count to 5.

- Due to current limitations in the Funk-Odyssey client software, clients cannot associate via a third-party APs or Bridges if xSec encryption is selected. (7684)
- xSec cannot be enabled on uplink trunk ports doing dot1q tagging. (7704)
- Some client NICs (for example, Dlink, 3Com) may experience problems sending frames when the MTU size exceeds 1408 bytes (7963)
- When a license key is installed, the system will inform the user that a reboot is necessary to enable the feature associated with the key. The license table will show that the key is enabled but there is no flag to indicate a reboot is required. (7845)
- The message: “Please reload the switch for the new service key to take effect” continues to display even after an existing temporary key is replaced with another temporary or permanent key. A reboot is not required if the associated feature is already enabled (as shown by the **show keys** CLI command or on the WebUI license management page). (7214)
- The message: “Reboot Cause: License Expired” displays with the **show switchinfo** CLI command output, but does not specify which of the licenses has expired and caused a scheduled system reboot. (7215)
- No SNMP traps are generated when software feature licenses are added, deleted, or expire. Syslog messages, however do report these events.(7450)
- The default configuration setting for certain software features (Intrusion Detection & Prevention, Policy Enhancement Firewall, etc) are not available when the associated keys are installed for the first time. (7555)
- When Offline RF Plan is newly installed on a Windows XP-SP2 machine, the error message: Can't create XMLHttpRequest object:Automation server can't create object" may appear. This message can be ignored and once the RF Plan page displays, this message will go away. (7965)
- Sygate SMS does not return MPPE keys when user authentication fails and host authentication is passed. (7736)
- When Sygate Virtual Desktop check is enabled, the first check will always fails and the subsequent check will pass. (7501)
- When two APs, wired APs, or Air Monitors configured are registered to the switch with the same location ID, and one of them is subsequently disconnected, the erroneous entry does not consistently clear in the WebUI. (7638)

Upgrading or Downgrading

If the software upgrade distributed with these release notes is on CD or some other static media, be sure to go to the Customer Support website to make sure you have the latest release of ArubaOS.

For information on upgrading to, or downgrading from, 2.4.0.0, refer to Installing ArubaOS 2.4.0.0—Prerequisites.

Before you Change your Switch’s Image

All Aruba Mobility Controllers store critical configuration data on an onboard Compact Flash memory module. In order to maintain the reliability of your Aruba WLAN network, Aruba recommends the following general best practices with respect to the use of your Aruba switch and its Compact Flash memory:

Backing up Critical Data

It is important to back up frequently all critical configuration data and files on Compact Flash file system to an off-switch external server or mass storage facility. At the very least, you should include the following files in these frequent off-switch backups:

- Configuration Data

- WMS Database
- Local User Database
- Licensing Database
- Floor Plan JPEGs
- Customer Captive Portal Pages
- Customer x.509 Certificates

Managing Flash Memory

Be careful not to exceed the size of the flash file system. For example, loading multiple large building JPEGs for RF Plan can consume the flash space quickly. Warning messages will alert you that the file system is running out of space whenever any write attempt to Flash occurs once there is 5Mbytes or less of space remaining.

Other tasks which are sensitive to insufficient Flash file system space include:

- Using the internal database - DHCP lease/renew information etc. is also stored on Flash. If the file system is full, DHCP addresses will not be distributed/renewed.
- If an Aruba switch encounters a bug where it needs to write a core file, it will not be able to do so if the file system is full and critical troubleshooting information will be lost.

Powering the System Down or Power Cycling the System

Compact Flash devices can be corrupted if power is lost during a write event (for example. **write mem**). To reduce the exposure of Compact Flash to corruption, be sure to follow these procedures:

For AirOS release 2.2 or greater:

- To power down:
    - From the CLI, type: **halt**.
    - The switch will respond with the message: **system halted**.
    - Now the switch is ready to be powered down or reset (at this point will automatically reset after approximately 90 seconds).

For releases prior to AirOS 2.2:

- To power down:
    - From the CLI type **reload**
    - Linux will shut down and when you see **Hit any key to stop autoboot**:, press Enter.
    - You are now at the cpboot prompt (cpboot>) and the switch is ready to be powered down or reset.

Installing ArubaOS 2.4.0.0—Prerequisites

- Make sure you have at least 10MB free flash.
- Back up the WMS database and TFTP it off the switch.
- Remove all unnecessary saved files from flash.
- Run the tar crash command to make sure that there are no "process died" files clogging up memory and TFTP the files off the switch.

Upgrading to ArubaOS 2.4.0.0

The Aruba ArubaOS software can be upgraded as new releases become available. The following steps abbreviate the detailed procedures located in the *Aruba ArubaOS 2.4 User's Guide*.

Caution — When upgrading the software in a multi-switch network (one that uses two or more Aruba Mobility Controllers), special care must be taken to upgrade all the Mobility Controllers in the network and to upgrade them in the proper sequence (see Upgrading Multi-Switch Networks

1. Obtain the latest, valid Aruba Mobility Controller software image from Aruba Customer Support.

Note— The most current Aruba Mobility Controller software image may be newer than that available at the time these release notes were written. Aruba recommends that you always download the latest software image from Aruba Customer Support before proceeding with these installation instructions.

2. Upload the new software image to a TFTP server on your network.
3. Verify the network connection between from the target switch to the TFTP server:

```
(aruba) # ping <TFTP server IP address>
```

4. Backup your current switch configuration.

   Use the following command to determine the name of your configuration file:

```
(aruba) # show boot
Config File: default.cfg
Boot Partition: PARTITION 0
```

   In this example, `default.cfg` is the configuration filename. To copy the configuration file to an external TFTP server, use the following command:

```
(aruba) # copy flash: default.cfg tftp: <TFTP server IP address> <dest. filename>
```

Note— A valid IP route must exist between the TFTP server and the Mobility Controller. Also required, a placeholder file with the destination filename and proper write permissions must exist on the TFTP server prior to executing the copy command.

5. Backup your current WMS and local user databases.

   Use the following commands to export the Mobility Controller's internal databases to an internal file with the filename of your choice, and then to an external TFTP server:

```
(aruba) # wms export-db <filename for WMS db>
(aruba) # copy flash: <filename for db> tftp: <TFTP server IP address> <dest. filename>
(aruba) # local-userdb export <filename for local user db>
(aruba) # copy flash: <filename for db> tftp: <TFTP server IP address> <dest. filename>
```

Note— A valid IP route must exist between the TFTP server and the Mobility Controller. Also required, a placeholder file with the proper write permissions for each destination filename must exist on the TFTP server prior to executing the copy commands.

6. Determine which memory partition will be used to hold the new software image.

   Use the following command to check the memory partitions:

```
(aruba) # show image version
---------------------------------
Partition               : 0:0 (/dev/hda1) **Default boot**
Software Version        : 2.4.0.0
Build number            : 10250
Built on                : Fri Apr 29 05:52:19 PDT 2005
---------------------------------
Partition               : 0:1 (/dev/hda2)
/dev/hda2: Image not present
---------------------------------
Partition               : 1:0 (/dev/hdc1)
Not plugged in.
---------------------------------
Partition               : 1:1 (/dev/hdc2)
Not plugged in.
```

   It is recommended to load the new image into the backup partition. In the above example, partition 0 contains the active image. Partition 1 is empty (`image not present`) and can be used for loading the new software.

7. Use the **copy** command to load the new image into the Aruba Mobility Controller:

   # **copy tftp:** <*server address*> <*image filename*> **system: partition** {**0**|**1**}

Note— When using the copy command to load a software image, the specified partition automatically becomes active the next time the switch is rebooted. There is no need manually select the partition.

8. Verify that the new image is loaded:

   # **show image version**

   Information about the newly loaded software image should be displayed for the appropriate partition.

9. Reboot the switch:

   # **reload**

10. When the boot process is complete, use the **show version** command to verify the upgrade.

```
(aruba) #show version
Aruba Wireless Operating System Software.
ArubaOS (MODEL: Aruba5000), Version 2.4.0.0
Website: http://www.arubanetworks.com
Copyright (c) 2003-2005 by Aruba Wireless Networks, Inc.
Compiled on 2005-1-1 at 15:02:41 PDT (build 8xxx) by p4build

ROM: System Bootstrap, Version CPBoot 1.0.6 (Aug 13 2003 - 16:17:05)

Switch uptime is 3 days 46 minutes 47 seconds
Reboot Cause: User reboot.
Aruba Supervisor Card
Aruba Processor (revision 16.20 (pvr 8081 1014)) with 256M bytes of
memory.
32K bytes of non-volatile configuration memory.
128M bytes of Supervisor Card System flash (model=TOSHIBA THNCF128MBA).



(aruba) #
```

   In this example, version 2.4.0.0 is loaded and running, indicating that the upgrade is complete.

11. Log in as the administrator and set the proper time zone for your location.

   (config) # **clock timezone** <*name of timezone*> <*UTC offset*>

Upgrading Multi-Switch Networks

In a multi-switch network (one with two or more Mobility Controllers), special care must be taken to upgrade all switches in the proper sequence, based on the switch type (master or local). Be sure to back up all switches being upgraded.

1. Make sure you have at least 10MB free flash.
2. Back up the WMS database and TFTP it off the switch.
3. Remove all unnecessary saved files from flash.
4. Run the tar crash command to make sure that there are no "process died" files clogging up memory and TFTP the files off the switch.

Upgrading to ArubaOS 2.4.0.0

Upgrading an Existing Network

To upgrade an existing multi-switch system to ArubaOS 2.4.0.0:

1. Upgrade the master Mobility Controller first.
2. Upgrade all local Mobility Controllers last.

Note— For proper operation, all Mobility Controllers in the network must be upgraded to use the same version of ArubaOS software.

Upgrading Redundant Switches

When configuring master/local switches in a redundant (VRRP) environment, the redundant switches should be the same class of switch (5000, 2400, or 800) or better, running the same revision of ArubaOS.

1. Aruba recommends upgrading in the following order:
2. Upgrade the Master switch to the new code.
3. Reboot the Master switch.
4. Upgrade the Local switches to the new code.
5. Do not reboot the Local switches yet.
6. From the Master CLI, enter
   `apboot location 0.0.0`
7. Now reboot the Local switches.

The APs should now have the new version of ArubaOS since they were rebooted and not failed over through VRRP.

Reverting to AirOS 2.X.X.X

If necessary, you can to return to your previous version of AirOS 2.X.X.X software after upgrading to a newer version. Be sure to back up your switch before reverting the OS. Also import the local database and the WMS database.

Caution — When reverting the Mobility Controller software, whenever possible use the previous version of software known to be used on the system. Loading a different prior release not specifically confirmed to operate in your environment could result in an improper configuration.

1. Determine the name of the current configuration file.

```
(aruba) #show boot
Config File: default.cfg


Boot Partition: PARTITION 1
```

In this example, `default.cfg` is the name of the configuration file.

2. Determine where your backup software is stored.

Use the following command to check the memory partitions:

```
(aruba) #show image ver
---------------------------------
Partition               : 0:0 (/dev/hda1)
Software Version        : 2.2.3.0
Build number            : 8096
Label                   : 8096
Built on                : 2004-07-07 01:26:15 PDT
---------------------------------
Partition               : 0:1 (/dev/hda2) **Default boot**
Software Version        : 2.4.0.0
Build number            : 10250
Label                   : 10250
Built on                : 2005-4-29 15:02:41 PDT
---------------------------------
Partition               : 1:0 (/dev/hdc1)
Not plugged in.
---------------------------------
Partition               : 1:1 (/dev/hdc2)
Not plugged in.
```

In this example, partition 0, contains the AirOS 2.2.3.0 backup. Partition 1, the active partition, contains the ArubaOS 2.4.0.0 image.

To select the backup partition as the new boot partition:

```
# boot system partition 0
```

3. If you have your backup configuration file on an external TFTP server, use the following command to copy it to the switch:

   # **copy tftp:** <*TFTP server IP address*> <*backup filename*> **flash:** <*backup configuration filename*>

4. Boot to your backup file as you cannot overwrite the active configuration file.

   # **boot config** <*backup configuration filename*>

5. Then replace the current configuration file with your backup.

   # **copy flash:** <*backup configuration filename*> **flash:** *default.cfg*

6. Boot to your `default.cfg` file.

   # **boot config** *default.cfg*

7. Replace the current WMS database file with your backup.

   If you have your backup database file on an external TFTP server, use the following commands to import it:

   # **copy tftp:** <*TFTP server IP address*> <*backup wms filename*> **flash:** <*wms filename*>

   # **wms import-db** <*wmsfilename*>

   If no backup image is present, load one:

   # **copy tftp:** <*server address*> <*image filename*> **system: partition** {**0**|**1**}

8. Select the backup partition as the new boot partition:

   # **boot system partition** {**0**|**1**}

9. Reboot the switch:

   # **reload**

10. When the boot process is complete, verify that the switch is using the correct software:

    # **show version**

Note— When reverting from ArubaOS 2.4.0.0 to AirOS 2.2.3.0 or earlier, all virtual APs that were provisioned in release 2.4.0.0 will have to be reprovisioned.

Troubleshooting

If the switch gets into trouble (for example, insufficient – less than 10MB – flash space), do the following:

1. Disconnect the link to the APs.

2. Remove all unnecessary files from flash, including the db_dump.sql type files.

3. Remove any crash files.
4. Import the old wms DB file and reboot.
5. Reconnect the link for the APs.

Documents in this Release

The following documents are included in this release:

- 050016-02 Software License Agreement
- 050021-03 Aruba 800 Wireless LAN Switch Installation Guide
- 050024-03 Aruba 5000/6000 Series Wireless LAN Switch Installation Guide
- 050025-03 Aruba 2400 Wireless LAN Switch Installation Guide
- 050030-02 Aruba RF Plan, Windows 2000/XP User's Guide
- 050034-05 Aruba AP 60/61 Installation Guide
- 050036-03 Aruba ArubaOS 2.4, User Guide
- 050037-03 Aruba AP 60/61 Mounting Kit Installation Guide
- 050039-03 Aruba ArubaOS V2.4 Message Reference
- 050041-03 ArubaOS Quick Start Guide
- 050042-02 Aruba 200W Power Supply Installation Guide
- 050043-02 Aruba 400W Power Supply Installation Guide
- 050044-02 Aruba AP 70 Installation Guide
- 050046-02 Aruba AP Enclosure Installation Guide
- 050047-02 Aruba Fan Tray Assembly Installation Guide
- 050048-02 Aruba 5000 SC Installation Guide
- 050049-02 Aruba 5000 LC Non-SPOE Installation Guide
- 050050-02 Aruba 5000 LC w/SPOE Installation Guide
- 050051-02 GBIC Installation Guide
- 050054-02 ArubaOS 2.4 Wireless Setup Map
- 050055-02 Aruba 2.4 Reference
- 050056-02 Aruba AP 70 Mounting Kit Installation Guide
- 050059-02 Aruba MIB Reference
- 050068-02 Aruba LC II Installation Guide
- 050092-02 Aruba 5000 Series LC-5000-2GE Installation Guide
- 050094-02 Aruba 6000 Series Supervisor Card Installation Guide
- 050095-02 Aruba 2E WIRED Access Point Installation Guide
- 050097-01 ArubaOS 2.4.0.0 Release Notes
- 050100-01 License Document Install Guide
- 050110-01 Aruba 800-E Wired Access Point Installation Guide
- 050111-01 Aruba 2400-E Wired Access Point Installation Guide

This documentation library is updated continuously. You can download the latest version of any of these documents from:

https://support.arubanetworks.com

For More Information

To contact Aruba Wireless Networks, refer to the information below:

Address

1322 Crossman Avenue

Sunnyvale, CA 94089

Phone

408 227 4500 (main)

408 227 4550 (fax)

Email

info@arubanetworks.com

Website

www.arubanetworks.com

Support

Phone:

US Toll Free: 1 800 WiFiLan (1 800 943 4526)
International: 1 408 754 1200

Email:

support@arubanetworks.com

Website:

http://www.arubanetworks.com/support